S04p/021W000

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平１１－２０３２４９

(43)公開日　平成１１年（１９９９）７月３０日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
G06F 15/00	330		G06F 15/00	330 D	
G09C 1/00	660		G09C 1/00	660 E	
H04L 9/32			H04L 9/00	673 B	
12/46				675 A	
12/28			11/00	310 C	

審査請求　未請求　請求項の数１０　ＯＬ　（全１７頁）　最終頁に続く

(21)出願番号　特願平１０－６３８５

(22)出願日　平成１０年（１９９８）１月１６日

(71)出願人　０００００５４９６
富士ゼロックス株式会社
東京都港区赤坂二丁目１７番２２号

(72)発明者　佐々木　茂彦
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　桂林　浩
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

(72)発明者　田丸　恵理子
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内

(74)代理人　弁理士　澤田　俊夫

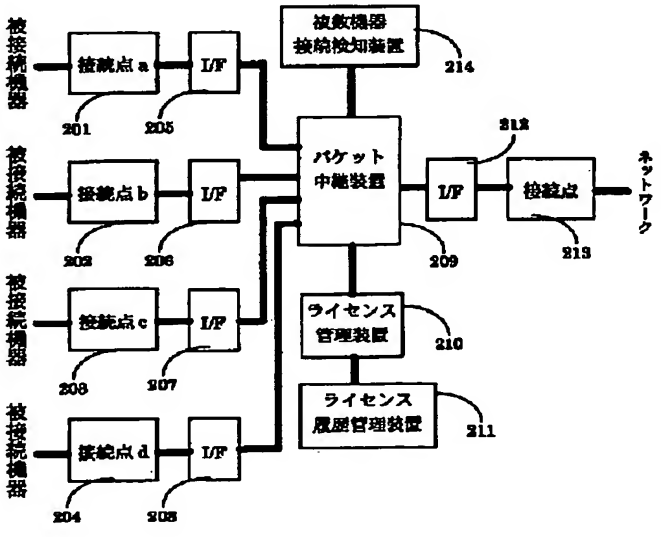
最終頁に続く

(54)【発明の名称】ライセンス付与システムおよびライセンス付与方法

(57)【要約】

【課題】　不特定多数の利用者が各自のＰＣ等の個人端末を利用して情報通信サービスを受ける形態において適切なライセンス付与を可能としたライセンス付与装置およびライセンス付与方法を提供する。

【解決手段】　データを中継するパケット中継装置２０９と、ネットワークアダプタ接続点２０１に接続される通信端末に対してライセンスの付与を実行するライセンス管理装置２１０とを有する。ライセンス管理装置２１０は、接続点２０１を介して接続された接続通信端末に対して、接続点固有の識別情報を送信し、次いで接続点固有の識別情報を受信した接続通信端末において該識別情報に基づいて生成されるデータを受信する。さらに、該受信データに基づいてレスポンスデータを生成し、該レスポンスデータの接続通信端末への送信を実行することによって接続通信端末に対するライセンス付与を行う。



1

【特許請求の範囲】

【請求項１】　通信端末を接続可能なネットワークアダプタ接続点を有し、該ネットワークアダプタ接続点に接続された通信端末に対して情報を提供する情報提供サービスに対する利用ライセンスの付与を実行するライセンス付与システムであり、

前記ネットワークアダプタ接続点を介して転送されるデータを中継するパケット中継装置と、

前記ネットワークアダプタ接続点に接続される通信端末に対してライセンスの付与を実行するライセンス管理装置とを備え、

前記ライセンス管理装置は、前記ネットワークアダプタ接続点を介して接続された接続通信端末に対して、該ネットワークアダプタ接続点固有の識別情報を送信するとともに、該ネットワークアダプタ接続点固有の識別情報を受信した前記接続通信端末において該識別情報に基づいて生成されるデータを受信し、該受信データに基づいてレスポンスデータを生成し、さらに該レスポンスデータの前記接続通信端末への送信を実行することによって接続通信端末に対するライセンス付与を行う構成を有することを特徴とするライセンス付与システム。

【請求項２】　前記ライセンス付与システムは、外部ネットワークに接続可能なネットワーク接続点を有し、

前記ライセンス付与システムの管理する前記ネットワークアダプタ接続点に接続された通信端末に対して、前記外部ネットワークから前記ネットワーク接続点を介して情報を提供する情報提供サービスに対する利用ライセンスの付与を実行する構成を有することを特徴とする請求項１記載のライセンス付与システム。

【請求項３】　前記ネットワークアダプタ接続点固有の識別情報は、該ネットワークアダプタ接続点固有の秘密鍵情報識別子であり、

前記通信端末において前記識別情報に基づいて生成されるデータは、少なくとも前記秘密鍵情報識別子を要素とする演算により生成されるチャレンジデータであり、

前記レスポンスデータは、少なくとも前記ネットワークアダプタ接続点固有の秘密鍵情報および前記チャレンジデータを要素とする演算により生成されるレスポンスデータであることを特徴とする請求項１または２に記載のライセンス付与システム。

【請求項４】　前記ライセンス付与システムは、さらに、前記接続通信端末に対するライセンス付与の履歴を記録するライセンス履歴管理装置を有し、

該ライセンス履歴管理装置は、前記ネットワークアダプタ接続点の各々に対するライセンス付与の実績を個々に記録した履歴データを生成する構成を有することを特徴とする請求項１乃至３いずれかに記載のライセンス付与システム。

【請求項５】　前記ライセンス付与システムは、前記ネットワーク接続点を介して実行される前記履歴データの

2

取得要求に対して、前記履歴データを暗号化して送付する構成を有し、

前記ライセンス付与システムは、前記ネットワーク接続点を介して要求された履歴データ取得要求に対して認証処理を実行し、該認証処理の成功を条件として前記履歴データ対する暗号化処理を行って、該暗号化履歴データの送付を行う構成を有することを特徴とする請求項４に記載のライセンス付与システム。

【請求項６】　前記ライセンス付与システムは、さらに単一のネットワークアダプタ接続点に複数のホストが接続されていることを検知する複数機器接続検知装置を有し、

前記複数機器接続検知装置による複数機器接続が検知された際には、該ネットワークアダプタ接続点に対するライセンス付与を停止する構成を有することを特徴とする請求項１乃至５いずれかに記載のライセンス付与システム。

【請求項７】　前記複数機器接続検知装置による複数機器接続の検知は、エコーパケットの送受信によって実行されることを特徴とする請求項６に記載のライセンス付与システム。

【請求項８】　前記ライセンス管理装置および前記パケット中継装置は一体化した構成を有し、

前記ライセンス管理装置の前記ライセンス付与システムからの切り離しにより前記パケット中継装置の機能が停止する構成を有することを特徴とする請求項１乃至７いずれかに記載のライセンス付与システム。

【請求項９】　通信端末を接続可能なネットワークアダプタ接続点を有し、該ネットワークアダプタ接続点に接続された通信端末に対して情報を提供する情報提供サービスに対する利用ライセンスの付与を実行するライセンス付与システムにおけるライセンス付与方法において、

前記ネットワークアダプタ接続点を介して接続された接続通信端末に対して、該ネットワークアダプタ接続点固有の識別情報を送信するステップと、

前記ネットワークアダプタ接続点固有の識別情報を受信した前記接続通信端末において該識別情報に基づいて生成される端末データを受信するステップと、

該端末データに基づいてレスポンスデータを生成し、該レスポンスデータを前記接続通信端末へ送信するステップと、

を有することを特徴とするライセンス付与システムにおけるライセンス付与方法。

【請求項１０】　前記ネットワークアダプタ接続点固有の識別情報は、該ネットワークアダプタ接続点固有の秘密鍵情報識別子であり、

前記通信端末において前記識別情報に基づいて生成されるデータは、少なくとも前記秘密鍵情報識別子を要素とする演算により生成されるチャレンジデータであり、

前記レスポンスデータは、少なくとも前記ネットワーク

アダプタ接続点固有の秘密鍵情報および前記チャレンジデータを要素とする演算により生成されるレスポンスデータであることを特徴とする請求項９記載のライセンス付与システムにおけるライセンス付与方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク接続サービスにおけるユーザへのサービス提供のライセンス付与システムおよびライセンス付与方法に関する。特に、不特定のユーザが使用する可能性のある、例えば公共の場所のネットワーク接続サービスを利用する環境において、備えつけ、あるいは指定のＰＣ（パーソナル・コンピュータ）を用いず、各利用者が個々のＰＣを持参し、持参ＰＣを接続してサービスを受けるような形態において不特定多数のユーザに適正にライセンスを付与するシステムおよび方法に関する。

【０００２】

【従来の技術】従来、ネットワーク接続サービスを利用するユーザに対するサービス利用の許諾、例えばサービス提供者の管理する特定のソフトウェアなどのデジタルコンテンツの使用ライセンスは、その情報サービスの提供を受けようとするユーザである人間を識別するか、あるいはユーザの使用するＰＣ等の機械を特定して、識別されたユーザ、あるいは使用端末に対してライセンスを付与することが一般的であった。

【０００３】ネットワーク接続サービス提供者からサービス利用のライセンスを付与されたユーザにはユーザを識別するための識別番号等のユーザＩＤ、また使用端末に対してライセンスが許諾された場合には、端末に対する識別番号等の端末ＩＤが付与され、サービスを受けようとするユーザは、識別番号等のユーザＩＤとともに、例えば利用者とサービス提供者との間で予め定められた所定のパスワードを入力することによってサービス提供者のサービスを受けることが可能となっているのが一般的である。

【０００４】しかし、例えばネットワークカフェ、公共の図書館、教育機関付属の共用計算機室など、多数の人間の出入りする公共の場所において不特定多数をサービス利用対象としてネットワーク接続サービスを提供する場合、従来のライセンス付与形態では問題がある。

【０００５】例えば、サービス利用者に対して利用者個々を識別可能なシリアル番号ＩＤ等のユーザＩＤを付与し、付与した個々のユーザＩＤに対応する電子チケット鍵によって、個々のユーザに対してライセンスを付与する技術（例えば特開平８－３３５１７０号公報に開示されている）では、ユーザを予め登録しておく会員制のサービスには対応可能であるが、不特定多数を対象にライセンスを付与することはできない。

【０００６】また、ユーザの保有するＩＣカードに秘密情報を記憶保持させて、ＩＣカードに対してライセンスを与える技術（例えば特開平８－１８６６６７号公報に開示されている）があるが、この技術もサービスの提供を望むユーザを会員制にして会員に秘密情報を保持させたＩＣカードを配付するか、不特定多数の人間が全員ＩＣカードを所持していることが期待できる環境でない限り、不特定多数を対象にライセンスを付与することができない。

【０００７】計算機、ＰＣ端末等の装置に固有な情報を利用して、計算機、ＰＣ端末等の装置に対してライセンスを付与する技術（特開平７－３２５７１２）を用いることにより、備えつけの計算機あるいはＰＣ等を用意して、その装置自体に対してライセンスを付与する形態をとることが可能となる。このような形態を整えれば計算機、あるいはＰＣ等、予め特定された端末を利用する不特定多数相手にライセンスを付与することができると考えられる。

【０００８】しかし、このような形態にも問題点がある。すなわち、公共の場所に設置してある不特定多数の人間が操作可能な計算機あるいはＰＣ等の端末を自由に操作可能とすることは、セキュリティの観点からは大変危険なことであるからである。なぜなら、備え付け端末のキーボードのタイプや通信内容の記録を取って窃用したり、あるいは悪意のプログラムを組み込む等、様々な操作を行う可能性が否定できないからである。

【０００９】そのため、今後は、自宅またはオフィス以外の例えば図書館等の公共機関においてサービスを受けようとする各利用者は、ポータブルＰＣや、ネットＰＣ、ＰＤＡを自ら持参し、公共機関に用意されたネットワークの接続点に接続して使用する形態が主流になることが予想される。この形態は、ユーザの持参した計算機、ＰＣ端末等を使用するので、悪意のプログラムが混入される心配はなく、また、普段使い慣れた環境で作業することができる利点がある。しかしながら、計算機、ＰＣ端末自体に対してライセンスを付与する技術では、使用する計算機、ＰＣ等を予め登録することが必要となるので、不特定多数相手にライセンスを付与することは困難である。

【００１０】以上、述べたとおり従来のライセンス付与技術では不特定多数の利用者が存在する図書館等、公共の場所におけるネットワーク接続サービスの提供において、備えつけＰＣを用いず、各利用者がＰＣ等を持参して持参ＰＣ等を接続端末として用いる形態での適切なライセンス付与が困難であり、特に、不特定多数の使用者にセキュリティを考慮した上でライセンスを付与することは困難であるという問題があった。

【００１１】

【発明が解決しようとする課題】本発明は、不特定の利用者が通信端末を利用した情報サービスを利用可能な例えば図書館等の公共の場所における通信ネットワーク接続サービスの利用において、セキュリティのために備え

5

つけのＰＣを利用しない形態で各自のＰＣ等の個人端末を利用した形態において不特定多数のサービス使用者に適切にライセンスを付与するライセンス付与装置およびライセンス付与方法を提供することを目的とする。

【００１２】

【課題を解決するための手段】本発明は、上述の目的を達成するライセンス付与システムであり、通信端末を接続可能なネットワークアダプタ接続点を有し、該ネットワークアダプタ接続点に接続された通信端末に対して情報を提供する情報提供サービスに対する利用ライセンスの付与を実行するライセンス付与システムであり、ネットワークアダプタ接続点を介して転送されるデータを中継するパケット中継装置と、ネットワークアダプタ接続点に接続される通信端末に対してライセンスの付与を実行するライセンス管理装置とを備え、ライセンス管理装置は、ネットワークアダプタ接続点を介して接続された接続通信端末に対して、該ネットワークアダプタ接続点固有の識別情報を送信するとともに、該ネットワークアダプタ接続点固有の識別情報を受信した接続通信端末において該識別情報に基づいて生成されるデータを受信し、該受信データに基づいてレスポンスデータを生成し、さらに該レスポンスデータの接続通信端末への送信を実行することによって接続通信端末に対するライセンス付与を行う構成を有することを特徴とする。

【００１３】さらに、本発明のライセンス付与システムは、外部ネットワークに接続可能なネットワーク接続点を有し、ライセンス付与システムの管理するネットワークアダプタ接続点に接続された通信端末に対して、外部ネットワークからネットワーク接続点を介して情報を提供する情報提供サービスに対する利用ライセンスの付与を実行する構成を有することを特徴とする。

【００１４】さらに、本発明のライセンス付与システムにおいて、ネットワークアダプタ接続点固有の識別情報は、該ネットワークアダプタ接続点固有の秘密鍵情報識別子であり、通信端末において識別情報に基づいて生成されるデータは、少なくとも秘密鍵情報識別子を要素とする演算により生成されるチャレンジデータであり、レスポンスデータは、少なくともネットワークアダプタ接続点固有の秘密鍵情報およびチャレンジデータを要素とする演算により生成されるレスポンスデータであることを特徴とする。

【００１５】さらに、本発明のライセンス付与システムは、さらに、接続通信端末に対するライセンス付与の履歴を記録するライセンス履歴管理装置を有し、該ライセンス履歴管理装置は、ネットワークアダプタ接続点の各々に対するライセンス付与の実績を個々に記録した履歴データを生成する構成を有することを特徴とする。

【００１６】さらに、本発明のライセンス付与システムは、ネットワーク接続点を介して実行される履歴データの取得要求に対して、履歴データを暗号化して送付する

6

構成を有し、ライセンス付与システムは、ネットワーク接続点を介して要求された履歴データ取得要求に対して認証処理を実行し、該認証処理の成功を条件として履歴データ対する暗号化処理を行って、該暗号化履歴データの送付を行う構成を有することを特徴とする。

【００１７】さらに、本発明のライセンス付与システムは、さらに単一のネットワークアダプタ接続点に複数のホストが接続されていることを検知する複数機器接続検知装置を有し、複数機器接続検知装置による複数機器接続が検知された際には、該ネットワークアダプタ接続点に対するライセンス付与を停止する構成を有することを特徴とする。

【００１８】さらに、本発明のライセンス付与システムにおいて、複数機器接続検知装置による複数機器接続の検知は、エコーパケットの送受信によって実行されることを特徴とする。

【００１９】さらに、本発明のライセンス付与システムにおいて、ライセンス管理装置およびパケット中継装置は一体化した構成を有し、ライセンス管理装置のライセンス付与システムからの切り離しによりパケット中継装置の機能が停止する構成を有することを特徴とする。

【００２０】さらに、本発明のライセンス付与方法は、通信端末を接続可能なネットワークアダプタ接続点を有し、該ネットワークアダプタ接続点に接続された通信端末に対して情報を提供する情報提供サービスに対する利用ライセンスの付与を実行するライセンス付与システムにおけるライセンス付与方法において、ネットワークアダプタ接続点を介して接続された接続通信端末に対して、該ネットワークアダプタ接続点固有の識別情報を送信するステップと、ネットワークアダプタ接続点固有の識別情報を受信した接続通信端末において該識別情報に基づいて生成される端末データを受信するステップと、該端末データに基づいてレスポンスデータを生成し、該レスポンスデータを接続通信端末へ送信するステップとを有することを特徴とする。

【００２１】さらに、本発明のライセンス付与方法において、ネットワークアダプタ接続点固有の識別情報は、該ネットワークアダプタ接続点固有の秘密鍵情報識別子であり、通信端末において識別情報に基づいて生成されるデータは、少なくとも秘密鍵情報識別子を要素とする演算により生成されるチャレンジデータであり、レスポンスデータは、少なくともネットワークアダプタ接続点固有の秘密鍵情報およびチャレンジデータを要素とする演算により生成されるレスポンスデータであることを特徴とする。

【００２２】

【発明の実施の形態】以下、本発明のライセンス付与システムの実施例について図面を参照して説明する。図１に本発明に係るライセンス付与システムの基本構成を表すブロック図を示す。

【００２３】図１のライセンス付与システムの構成について説明する。図１に示すライセンス付与システムの左端はＰＣ等の接続端末が接続可能な構成を有し、一方、ライセンス付与システムの右端はサービス提供者、あるいは履歴データ回収センター等にネットワークを介して接続可能な通信ネットワークに接続する構成を有する。図１に示すライセンス付与システムは、接続点１０１と、Ｉ／Ｆ（インタフェース）１０２，１０５と、パケット中継装置１０３と、ライセンス付与装置１０４と、接続点１０６から構成される。以下、ライセンス付与システムを構成する各構成要素について説明する。

【００２４】接続点１０１はＰＣ等の被接続機器に接続するネットワークアダプタ接続点であり、Ｉ／Ｆ（インタフェース）１０２はライセンス付与システム内部と接続点１０１に接続されるＰＣ等の接続機器との電気的整合をとる電気的インタフェースであり、パケット中継装置１０３は、被接続機器であるＰＣと外部ＬＡＮの間に流れるデータを中継する。また、ライセンス付与装置１０４は、ライセンスの管理と付与の記録を行う機構を有する。Ｉ／Ｆ（インタフェース）１０５はライセンス付与システム内部と外部のネットワークとの電気的整合をとる電気的インタフェースであり、接続点１０６は、ライセンス付与システムと外部のネットワークとを接続する。

【００２５】さらに、本発明のライセンス付与システムは複数の被接続機器に対応するため、図２に示す構成をとることが可能である。図２に示す構成例では、複数の被接続機器を接続可能とするために複数のネットワークアダプタ接続点として接続点ａ，２０１、接続点ｂ，２０２、接続点ｃ，２０３、接続点ｄ，２０４が設けられ、さらに、個々の接続点に対応して電気Ｉ／Ｆ（インタフェース）２０５、２０６、２０７、２０８が設けられている。また、各被接続機器と外部ＬＡＮの間に流れるデータを中継するパケット中継装置２０９と、ライセンスを付与するライセンス管理装置２１０と、ライセンス付与の履歴をとるライセンス履歴管理装置２１１と、外部のネットワークの電気Ｉ／Ｆ（インタフェース）２１２と、外部のネットワークに接続される接続点２１３と、ひとつのネットワークアダプタ接続点に、ハブ装置などで複数の機器を接続したことを検知する複数機器接続検知装置２１４から構成される。

【００２６】この図２に示すライセンス付与システムの例では被接続機器を接続するネットワークアダプタ接続点を４つ持つが、これらネットワークアダプタ接続点は、さらに増加させることも、または減少させることも可能であり、ライセンス付与システムおよび接続機器の利用形態に応じた接続点数を設定してシステム構築することができる。

【００２７】以下、本発明のライセンス付与システムの動作について、図２に示すライセンス付与システム構成例中の各構成要素の機能を中心に説明する。なお、図１に示すシステムも同様に動作するものである。

【００２８】ネットワークアダプタ接続点（接続点ａ，２０１～接続点ｄ，２０４のいずれか）から発信されたパケットは、本発明のライセンス付与システム中のパケット中継装置２０９によって指定されるパケットの宛先に応じて、外部ネットワークまたは他のネットワークアダプタ接続点に中継される。

【００２９】また、外部ネットワークから接続点２１３を介してライセンス付与システムに接続されたＰＣ端末等の被接続機器宛のパケットが届いたときは、パケット中継装置２０９によって宛先として指定された対象の被接続機器が接続されたネットワークアダプタ接続点（接続点ａ，２０１～接続点ｄ，２０４のいずれか）にパケットの中継がなされる。つまり、パケット中継装置２０９は従来のスイッチングハブ（例えば、特開平５－３００１６５に開示されている。）の機能を兼ね備える。

【００３０】図２に示すライセンス付与システムの例では、ライセンス管理装置２１０とライセンス履歴管理装置２１１は、別ブロックとして構成して示してあるが、これらの両装置は一体のシステムとして構成することも可能である。図３は、ライセンス管理装置２１０とライセンス履歴管理装置２１１とを併せて構成した例を示す構成ブロック図である。

【００３１】ライセンス管理装置２１０とライセンス履歴管理装置２１１は、図２に示す接続点ａ，２０１～接続点ｄ，２０４に接続された被接続機器からのライセンス付与の要求に対する応答、およびネットワークを介して接続されるサービス提供者からのライセンス履歴回収の要求に対する応答を行う。これらの機能を果たすために、ライセンス管理装置２１０とライセンス履歴管理装置２１１は、図３に示されるようにライセンス付与システム内の機器の制御を行う機器制御装置３０１、秘密鍵情報とライセンスの付与の履歴の記録を保持する記憶装置３０２、および任意の数を法数に設定できる整数の演算回路３０３を有する。

【００３２】また、図２に示すライセンス管理装置２１０およびパケット中継装置２０９は物理的に一体化した構成とすることが望ましく、これら両装置を一体化することでライセンス管理装置２１０をライセンス付与システムからの切り離した場合にパケット中継装置２０９の機能が停止する構成とし、不正なデータの取り出しを容易に発見可能とすることができる。

【００３３】図２に示すようにネットワークアダプタ接続点２０１と、ライセンス管理装置２１０、ライセンス履歴管理装置２１１は、パケット中継装置２０９を介して接続され、各接続点間および装置間のデータ転送がパケット中継装置２０９を介して可能な構成となっている。

【００３４】パケット中継装置２０９はスイッチング技

術によりパケットを中継することにより、各々の接続点ａ，２０１～接続点ｄ，２０４とライセンス管理装置２１０との間のパケットを、他の接続点と外部ネットワークからモニタさせることなく、安全に中継することができる。また、他の接続点や外部ネットワークから不正にライセンス管理装置２１０にアクセスすることも防止できる。

【００３５】パケット中継装置２０９の動作を詳しく説明する。パケット中継装置２０９はパケット中継装置内部の記憶装置に図４に示すような経路表をデータとして保持している。図４に示すように経路表には、ネットワーク機器のＭＡＣアドレス、経路先のポート番号、登録期限が記録される。また、ライセンス管理装置の経路は初期設定時に登録されており、登録期限は永遠（無期限）に設定される。図４に示す経路表の例では、ＭＡＣアドレスとして管理装置以外にひ接続装置１がポート番号「接続点ａ」に、ルータがポート番号「外部ネットワークのポート」として登録され、さらに、それぞれの登録期限が設定さている。パケット中継装置２０９は、この経路表に登録されたデータに基づいてパケットの適切な配信を実行する。

【００３６】図５はパケット中継装置２０９の動作を説明するフローチャートである。以下、図５に示すフローチャートに沿ってパケット中継装置２０９の動作を詳細に説明する。

【００３７】パケット中継装置２０９には、パケットを送信および受信するインタフェースが複数接続される。例えば、各ネットワークアダプタ接続点、外部ネットワーク接続点、ライセンス管理装置に対するインターフェースである。各インタフェースをポートといい、それぞれに一意なポート番号が割り当てられ、識別可能な構成となっている。

【００３８】フローチャートのステップ５０１にあるように、パケット中継装置２０９は、常時すべてのポートからくるパケットを監視している。いずれかのポートからのパケットを受信すると、ステップ５０２に処理を進める。

【００３９】ステップ５０２では、パケットを受信したポート番号と、発信元のＭＡＣアドレスの対応を経路表（図４参照のこと）に登録する。経路表登録時にあらかじめ定めた時間を加えた時刻を登録期限として経路表に登録する。登録期限は、前述のように例えばライセンス管理装置であれば無期限であるが、一般の接続端末の使用ポートであれば、例えば１時間、あるいは図書館等であれば図書館の閉館時間等、予め設定した期限を登録する。

【００４０】ステップ５０３において、パケットが、複数宛のブロードキャストまたはマルチキャストか、単一のホスト宛先のユニキャストかを判断する。複数宛のブロードキャストであった場合（ステップ５０３の判定がＹｅｓの場合）は、ステップ５０７（パケットの同時中継）に分岐する。単一ホスト宛である場合は、ステップ５０４に進む。

【００４１】先に、単一ホスト宛先であるユニキャストだった場合（ステップ５０３の判定がＮｏの場合）の説明をする。ステップ５０４では、宛先に指定されたＭＡＣアドレスが経路表に登録されているか判断する。もし経路表にＭＡＣアドレスが登録されていない場合には、ブロードキャストの場合と同様ステップ５０７に分岐する。ＭＡＣアドレスが経路表に登録されていた場合は、ステップ５０５に処理を進める。

【００４２】ブロードキャストでなく、経路表にＭＡＣアドレスが登録されている場合は、ステップ５０５で、パケットが発信されたポート番号と、経路表から検索した宛先のＭＡＣアドレスに対応するポート番号が同じかを判断する。もし同じだった場合には、中継する必要無しとして、処理を終える。異なった場合はステップ５０６に処理を進める。

【００４３】ステップ５０６では、経路表から得た宛先のポートに対して、パケットを中継する。

【００４４】ステップ５０７は、パケットがブロードキャストか、経路表に宛先が無い場合の処理である。パケットが発信されたポート以外のすべてのポートに対して、パケットを同時に中継する。

【００４５】以上説明したように、必要がないポートにパケットを中継しないことにより、通信路の輻輳を防ぎ、通信路を効率的に使用できるようにするとともに、関係のない通信路にパケットが中継されないことにより、宛先と異なるポートでのデータ傍受の危険性を防止する。

【００４６】特に、ライセンス管理システムの経路情報は永久的に経路表に登録されているため、必ず、パケットは必要な経路にしか中継されず、他のポートから通信内容を傍受することができないようになっている。

【００４７】図６は、ライセンス管理装置が送受信するパケットの構造である。最初の１バイトは、そのパケットの種類、たとえばクエリー、リプライ、チャレンジ、リスポンス等をあらわす。続く２ｂｙｔｅは、データ列部分の長さをあらわす。符号無し２進数で、重いビット（ＭＳＢ）から軽いビット（ＬＳＢ）という順番、いわゆるビッグエンディアン（Ｂｉｇ　Ｅｎｄｉａｎ）方式で格納される。長さが０の場合、データ列部は省略される。

【００４８】その後に、データ列部はデータの長さに指定された指定長だけ続く。特に、エラー検出、訂正用の符号は付加しない。ＴＣＰ／ＩＰのエラー訂正機能に依存している。

【００４９】図７に、ライセンス管理装置２１０とライセンス履歴管理装置２１１の処理の概略のフローチャートを示す。前述のようにライセンス管理装置２１０とラ

11

イセンス履歴管理装置２１１は、図２に示す接続点ａ，２０１～接続点ｄ，２０４に接続された被接続機器からのライセンス付与の要求に対する応答、およびネットワークを介して接続されるサービス提供者からのライセンス履歴回収の要求に対する応答を行う。

【００５０】以下に、図７に示すフローチャートに沿ってライセンス管理装置２１０の動作の説明をする。ステップ７０１では、ライセンス管理装置２１０は自分宛のパケットを待ち受ける。パケットを受信したらステップ７０２に処理を進める。ライセンス管理装置は、前述のようにすべてのポートを対象としてパケットを待機している。

【００５１】ステップ７０２では、パケットを受信したポートが、外部ネットワークのものかどうかを判断する。もし外部ネットワークのものであったならば、ライセンス付与プロトコルの応答はせず、ライセンス履歴管理装置２１１の履歴データの回収のみ対応する。フローチャート上では、ステップ７０８（接続先の認証）に処理を進める。もしネットワークアダプタ接続点（２０１～２０４）のポートであった場合には、ステップ７０３に処理を進め、受信ポートに対するライセンス付与を行う。

【００５２】続いてライセンス付与処理について説明する。本例では、ライセンス付与は公開鍵暗号系を元に作られた例えば特開平９－２０５４２４に開示された方法でライセンス付与、および暗号化されたコンテンツの実行の許可を行った。しかし、他の秘密鍵情報を必要とする暗号技術によるライセンス付与方式を用いても構わない。ライセンス管理装置２１０には各ポートに対応する秘密鍵情報を保持しており、ポートごとにライセンスを付与することができる。

【００５３】ステップ７０３では、パケットを受信したポートに対応する秘密鍵情報を記憶装置からロードし、その秘密鍵に対応するＩＤコードを最初のパケットを発信した機器に返信する。次いで、ステップ７０４で、被接続機器からチャレンジのパケットを受取る。チャレンジとは、意味のあるデータに、ある種の乱数で処理することにより回線を傍受されても安全なデータ列のことである。

【００５４】ステップ７０５で、受信したチャレンジと、秘密鍵を用いて演算を行い、レスポンスを生成する。

【００５５】次に、ステップ７０６において、対象機機のＭＡＣアドレス、ポート番号、時刻、チャレンジ等をライセンス履歴としてライセンス履歴管理装置２１１に記録する。

【００５６】ステップ７０７では、レスポンスを被接続機器に返信し、ライセンス付与処理を終了する。レスポンス単体では、チャレンジに施された乱数処理のために傍受されても構わないデータ列であるが、被接続機器側

12

では乱数処理に用いた乱数を保持しているため、レスポンスから意味のあるライセンス付与鍵に復元することができる。

【００５７】以上、説明したライセンス付与動作時のパケットのやりとりを図８に示す。図８について簡単に説明する。まずサービスを受けようとする被接続機器側からライセンス管理装置に対してクエリーパケットが送付される。すべてのポートからのパケットを待機しているライセンス管理装置は、このパケットを受信すると、そのパケットを送信したポートに対する秘密鍵情報ＩＤを記憶装置から取り出してポートに対して送信する。

【００５８】秘密鍵情報ＩＤを受信したポートは、サービスを受けようとするデジタルコンテンツＩＤ、チケット情報、乱数等によりチャレンジデータを生成し、これをライセンス管理装置に送信する。

【００５９】チャレンジデータを受信したライセンス管理装置は、チャレンジデータおよび秘密鍵情報に基づいて演算を実行し、レスポンスを生成する。生成されたレスポンスは、被接続機器に送付され、被接続機器では、受信レスポンスと乱数に基づいて暗号解読鍵、すなわちライセンス付与鍵を得る。

【００６０】次に、ライセンス付与の履歴データ回収の処理について説明する。図９は、ライセンス履歴管理装置２１１に保持されるライセンス履歴の構造である。ライセンス付与動作を行うたびに、１レコード行ずつ追記していく。レコード行は、連続番号、ライセンス付与した時刻、付与対象の接続機器のＭＡＣアドレスと、その機器が接続されているポート番号、付与時に受信したチャレンジのデータ列である。

【００６１】図７のステップ７０２で、ライセンス管理装置２１０が接続点２１３を介して外部ネットワーク側からパケットを受取ったと判断した場合には、ライセンス履歴回収の処理を行う。

【００６２】ステップ７０８は、接続先との認証を行うステップである。外部ネットワークには様々なネットワーク機器が接続されており、信用できない物も多く存在する。そのため、信用してもよいか否かを判定する認証処理を行う。本装置では、公開鍵暗号系の電子署名技術を用いて相手の認証を行う。もちろん別の方法で認証を行っても構わない。

【００６３】ステップ７０９で認証に失敗したと判断された場合、ステップ７１１でエラー処理を行い、処理を終了させる。認証に成功した場合は、ステップ７１０に進み、ライセンス履歴管理装置２１１から履歴データを送信する。

【００６４】本発明のライセンス付与システム中のライセンス履歴管理装置２１１から送信する履歴データには、暗号化処理と電子署名処理が行われ、傍受されても安全な構成となっている。暗号化されて正当な宛先に送付された暗号化履歴データは、復号鍵によって復号され

る。

【００６５】以上、説明したライセンス付与動作時のライセンス履歴管理装置２１１とネットワークに接続された例えばサービス提供者等の履歴回収センターとの間におけるパケットのやりとりを図１０に示す。

【００６６】図１０について簡単に説明する。まず履歴データを取得しようとする履歴回収センターからライセンス管理装置に対してネットワークを介してクエリーパケットが送付される。すべてのポートからのパケットを待機しているライセンス管理装置は、このパケットを受信すると、管理装置ＩＤを記憶装置から取り出して履歴回収センターに対して送信する。

【００６７】管理装置ＩＤを受信した履歴回収センターは、ログ回収時の暗号鍵を乱数から生成し、さらに電子署名を加えて認証パケットを生成して、これをライセンス管理装置に送信する。

【００６８】認証パケットを受信したライセンス管理装置は、履歴データを記憶装置から取り出し、暗号鍵によって暗号化して、これをパケットとして履歴回収センターに対して送信する。履歴回収センターでは、復号鍵によって受信した暗号化履歴データを復号し、履歴データを獲得する。

【００６９】次に、図２に示した複数機器接続検知装置２１４について、説明する。複数機器接続装置２１４は、一定時間おきに、各ネットワークアダプタ接続点に、エコーパケットをブロードキャストモードで送信する。エコーパケットとは、ＴＣＰ／ＩＰプロトコルのＩＣＭＰ（Ｉｎｔｅｒｎｅｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ　Ｐｒｏｔｏｃｏｌ）パケットの一種で、接続状態を確認するためのパケットである。

【００７０】ＩＰが実装された接続端末等の機器は、エコーパケットを受信したら、必ず返信パケットを送信する規約になっている。ＵＮＩＸやＷｉｎｄｏｗｓシステムのｐｉｎｇコマンドは、このエコー（ｅｃｈｏ）パケットを利用して、実装されている。

【００７１】複数機器中継装置２１４が発行するエコー（ｅｃｈｏ）パケットは、パケット中継装置２０９により中継されない。そのため、対象の接続点にのみパケットが送信される。

【００７２】図１１にあるように、一つの接続点にバス接続や分配機によって、複数の機器が接続されているとする。この接続点から、ブロードキャストモードで、エコー（ｅｃｈｏ）パケットを発信すると、接続されているすべての機器にエコー（ｅｃｈｏ）パケットが到達する。

【００７３】すると、図１２に示すように、各機器から返信エコー（ｅｃｈｏ）パケットが発信され、接続点では、接続された機器の数だけ返信エコー（ｅｃｈｏ）パケットが観測される。つまり、返信エコー（ｅｃｈｏ）パケット数を数えることにより、複数の機器がひとつの接続点に接続されていることを検知できる。

【００７４】不正ライセンス取得や機器間の通信内容の傍受を防止するため、ひとつの接続点に複数の機器の接続を検知したときは、異常接続が発生としたみなし、その接続点に関するライセンス付与機能を停止する。

【００７５】このような制限を加えることによって、複数の被接続機器に同じ秘密鍵に対応するライセンスを同時に付与することを防ぐことができ、また、被接続機器と本装置間の通信の傍受を防止することもできる。以上のように、本発明のライセンス付与装置によれば安全にライセンスを付与する構成が実現される。

【００７６】次に実際に本装置を用いて、公共の場所で、不特定多数を対象にライセンスを付与する状況の説明をする。説明は、モデルを用いて行う。以下に、説明のためのモデルの前提条件を挙げる。

【００７７】デジタル化された本や映画、インタラクティブメディアやゲームソフトなど、デジタルデータで構成され、容易に劣化しない複製ができる著作物をデジタルコンテンツと呼ぶ。有料のデジタルコンテンツが存在し、それらは、利用するたびに利用料を、著作権者、あるいはサービス提供者に支払う利用料課金システムを採用しているものとする。

【００７８】公共の場所として、公立図書館を想定する。この公立図書館は、住民サービスとして、デジタルコンテンツの利用料を、館内で利用する場合にかぎり、誰が利用するかに関わらず図書館が負担する。しかし、館外で利用される分については、図書館は負担しないので、利用者自身が支払う必要があるものとする。

【００７９】デジタルコンテンツは、特開平９－２０５４２４にあげられた方法で暗号化されているとする。コンテンツは、各タイトルそれぞれ別の暗号化鍵で暗号化される。また、利用するために必要な秘密鍵情報も、各利用者ごとに異なる秘密鍵情報が配付される。

【００８０】コンテンツを利用するためには、暗号化されたコンテンツと、利用側が保持する秘密鍵情報と、その暗号鍵と秘密鍵情報に対応したチケット情報の３つを揃える必要がある。

【００８１】暗号化されたコンテンツは、図書館のファイルサーバに保持されている必要は必ずしもなく、ネットワークでアクセス可能な場所であればどこにあっても構わない。秘密鍵情報は、本件の装置に保持される。チケット情報は、特開平９－２０５４２４にあげられた方法で流通を行う業者が発行する。

【００８２】この業者は、コンテンツの暗号化、秘密鍵情報の配付、チケット情報の発行の業務を行う。チケット情報を生成するためには、対象コンテンツの暗号鍵と対象ユーザの秘密鍵が必要で、これらの情報なくしてチケット情報を生成することはできない。

【００８３】本例では、サービス対象が不特定多数なため、図書館とコンテンツの著作者とのライセンス契約に

より、生成されたチケット情報は誰でも入手できる場所に公開される。

【００８４】以上が前提である。公立図書館には、デジタルコンテンツを利用閲覧するために、図１３に示すようなブースが用意される。各ブースには、本件の安全にライセンスを付与する装置のネットワークアダプタ接続点が設置してあり、ここにＰＣやＰＤＡ等のネットワーク機器を接続することにより、図書館内外のネットワークにアクセスすることができる。

【００８５】ユーザーは、自分で持ち込んだＰＣを接続点に接続する。ネットワークを介して、自分が利用したいデジタルコンテンツをダウンロードする。

【００８６】しかし、コンテンツは暗号化されているため、そのままでは利用することができない。

【００８７】まず、ＰＣから、ネットワークアダプタ接続点を介して、ライセンス管理装置に、ライセンスの付与をリクエストする。ライセンス管理装置からは、秘密鍵情報のＩＤ番号と、チケット情報の公開されている場所が返信される。

【００８８】ネットワークを介して、チケット情報をダウンロードし、チケット情報からチャレンジを生成、それをライセンス管理装置に送信する。ライセンス管理装置は、秘密鍵情報とチャレンジからレスポンスを生成、利用者のＰＣに返信する。利用者のＰＣは、受取ったレスポンスを用いて、暗号化されたコンテンツを解読し利用することができる。ただし、解読された状態のデータを保存することは禁止されており、解読されたデータは利用された直後にすぐに廃棄される。

【００８９】また、以上のやりとりは、履歴データに保存される。暗号化コンテンツの流通業者がネットワークを介して、各ライセンス管理装置から、ライセンス付与の履歴を回収、集計して図書館に利用料を請求する。

【００９０】利用者が暗号化されたコンテンツと、チケット情報をＰＣに保存して、図書館の外に出ても、館外では、秘密鍵情報にアクセスできないため、コンテンツを利用することができない。

【００９１】コンテンツを館外で利用するためには、利用者は暗号化コンテンツの流通業者と契約を結び、利用者は個人用の秘密鍵情報と、それに対応するチケットの配付を受けなくてはならない。もちろん利用料は利用者の負担である。

【００９２】また、秘密鍵情報の決まった場所からしかアクセスできないと言う特性は、逆に言うと、誰でもそのブースから秘密鍵情報にアクセスできるということで、不特定多数にサービスするのに適している。

【００９３】以上説明したように、ライセンス管理装置は動作する。そのため、各ポートごとに、異なる秘密鍵情報が割り当てられ、各ネットワークアダプタ接続点ごとにライセンスを付与することができる。

【００９４】また、ライセンス付与に関する付与システムおよび端末間における通信は、他の接続点から傍受することができないため、安全である。それに加え、ライセンス管理装置が常に外部ネットワークに接続されているため、容易に外部から、ライセンス管理装置にアクセスして、ライセンス管理の履歴情報をネットワークを介して回収することができる。

【００９５】物理的に、ライセンス管理装置は、パケット中継装置と一体に形成されているため、悪意により盗難や破壊が行われた場合、パケットが中継されなくなり、このような盗難あるいは破壊の際には、パケット中継の停止により、その事実が容易に発見される。

【００９６】

【発明の効果】以上説明したように本発明のライセンス付与システムおよびライセンス付与方法によれば、どのような接続マシンや利用者に対しても、ネットワークの接続点という場所属性に対応するライセンスを付与することが可能となる。このため、例えば公共の場所で不特定多数に対してライセンスを適正に付与することが可能となる。

【００９７】また、ライセンス付与システム装置内に秘密情報が固定されているため、解析が困難であり、また、内部の記憶装置を取り外すと、パケット中継機能も破壊されるため、内部情報に対する侵入がすぐに発覚するので、より効果的な機密漏洩防止が可能となる。

【００９８】また、本発明のライセンス付与システムおよびライセンス付与方法によれば、ライセンス付与システムがネットワークに常時接続可能にな構成を有し、外部の各機関からライセンス付与システムに対するアクセスが随時可能であり、またライセンス付与履歴をシステム中に記憶保持しているので、外部からの任意のタイミングでのアクセスにより容易にライセンス付与履歴を回収することができるという効果がある。

【図面の簡単な説明】

【図１】　本発明のライセンス付与システムの一実施例を示すブロック図である。

【図２】　本発明のライセンス付与システムの一実施例であり、複数の接続機器を接続可能とした構成例を示すブロック図である。

【図３】　複数のネットワークアダプタ接続点をもつライセンス付与システムのライセンス管理装置の構成を示す図である。

【図４】　本発明のライセンス付与システム中のパケット中継装置が有する経路表の構造例を示す図である。

【図５】　本発明のライセンス付与システムにおけるパケット中継装置の動作のフローを示す図である。

【図６】　本発明のライセンス付与システムにおけるライセンス管理装置が送受信するパケットの構造を示す図である。

【図７】　本発明のライセンス付与システムにおけるライセンス管理装置の動作のフロを示す図である。

17　　18

【図８】　本発明のライセンス付与システムにおけるライセンス付与動作におけるパケットのやりとりを示す図である。

【図９】　本発明のライセンス付与システムにおけるライセンス付与履歴のデータ構造を示す図である。

【図１０】　本発明のライセンス付与システムにおけるライセンス付与履歴の回収動作におけるパケットのやりとりを示す図である。

【図１１】　本発明のライセンス付与システムにおける複数機器接続検知装置の動作（ブロードキャスト・エコーパケット発信）を示す図である。

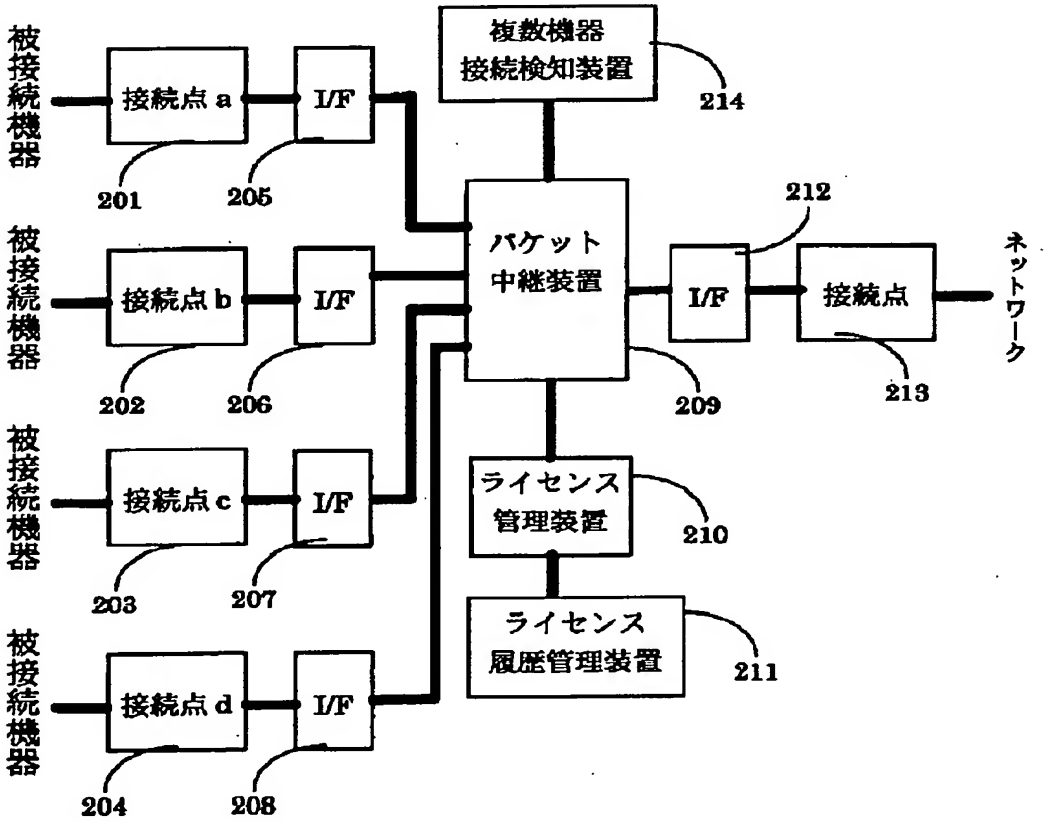
【図１２】　本発明のライセンス付与システムにおける複数機器接続検知装置の動作（返信エコーパケット受信）を示す図である。

【図１３】　公立図書館において本発明のライセンス付与システムを使用した場合の利用ブースの概念図である。

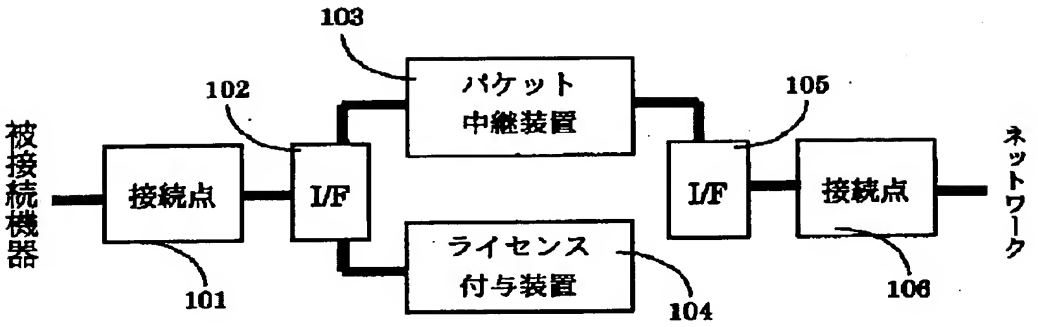
【符号の説明】

１０１，１０６　接続点
１０２，１０５　インタフェース
１０３　パケット中継装置
１０４　ライセンス付与装置
２０１，２０２，２０３，２０４，２１３　接続点
２０５，２０６，２０７，２０８，２１２　インタフェース
２０９　パケット中継装置
２１０　ライセンス管理装置
２１１　ライセンス履歴管理装置
２１４　複数機器接続検知装置
３０１　機器制御装置
３０２　記憶装置
３０３　演算装置

【図２】



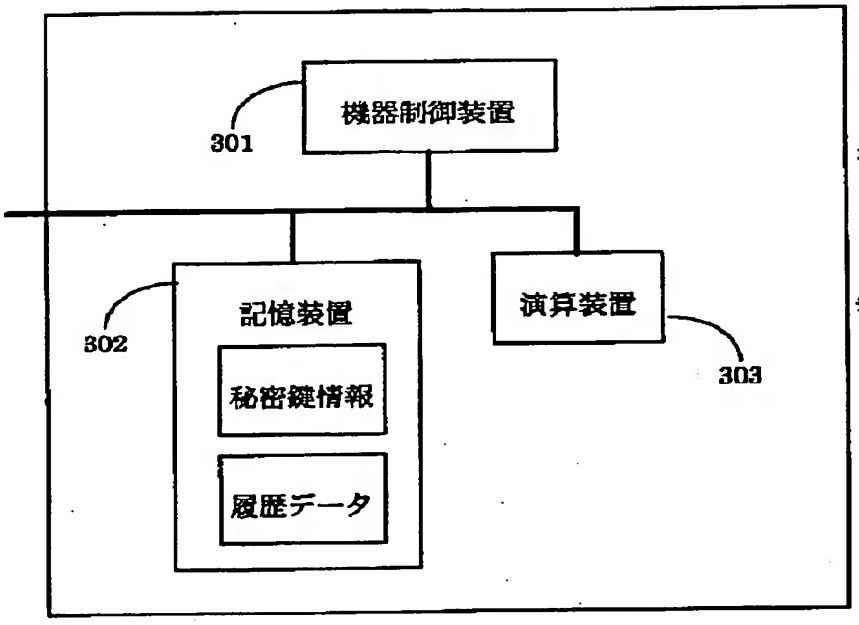
【図１】



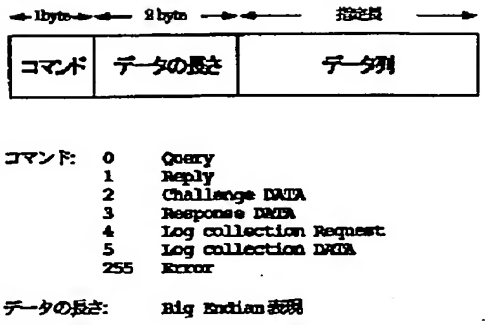
【図９】

S/N	ライセンス付与時刻	MACアドレス	ポート番号	チャレンジ データ列
1001	19970812 091132.22	被接続装置２	接続点 a	67433221....12321321
1002	19970813 051152.02	被接続装置１	接続点 b	54343433....22147852
1003				

【図３】



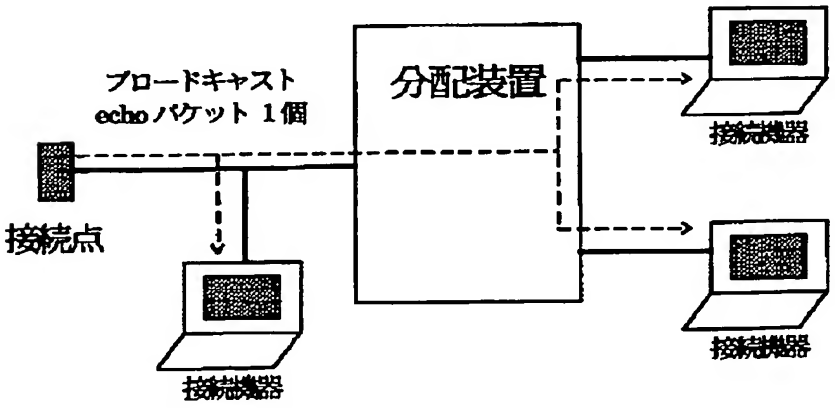
【図６】



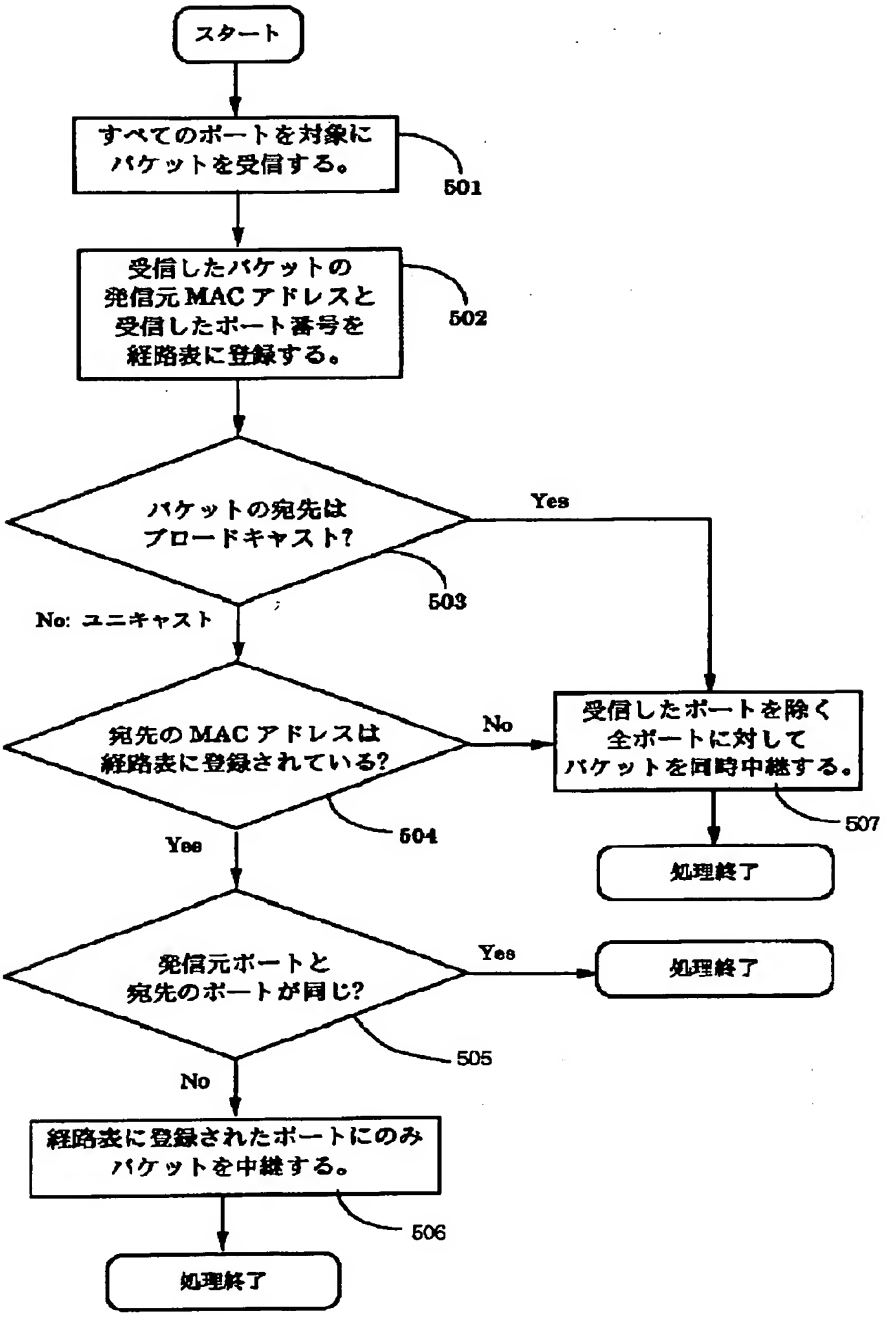
【図４】

MACアドレス	ポート番号	登録期限
ライセンス管理装置	ライセンス管理装置のポート	永遠
被接続装置１	接続点ａ	19970810 123407.12
ルータ	外部ネットワークのポート	19970810 092310.55

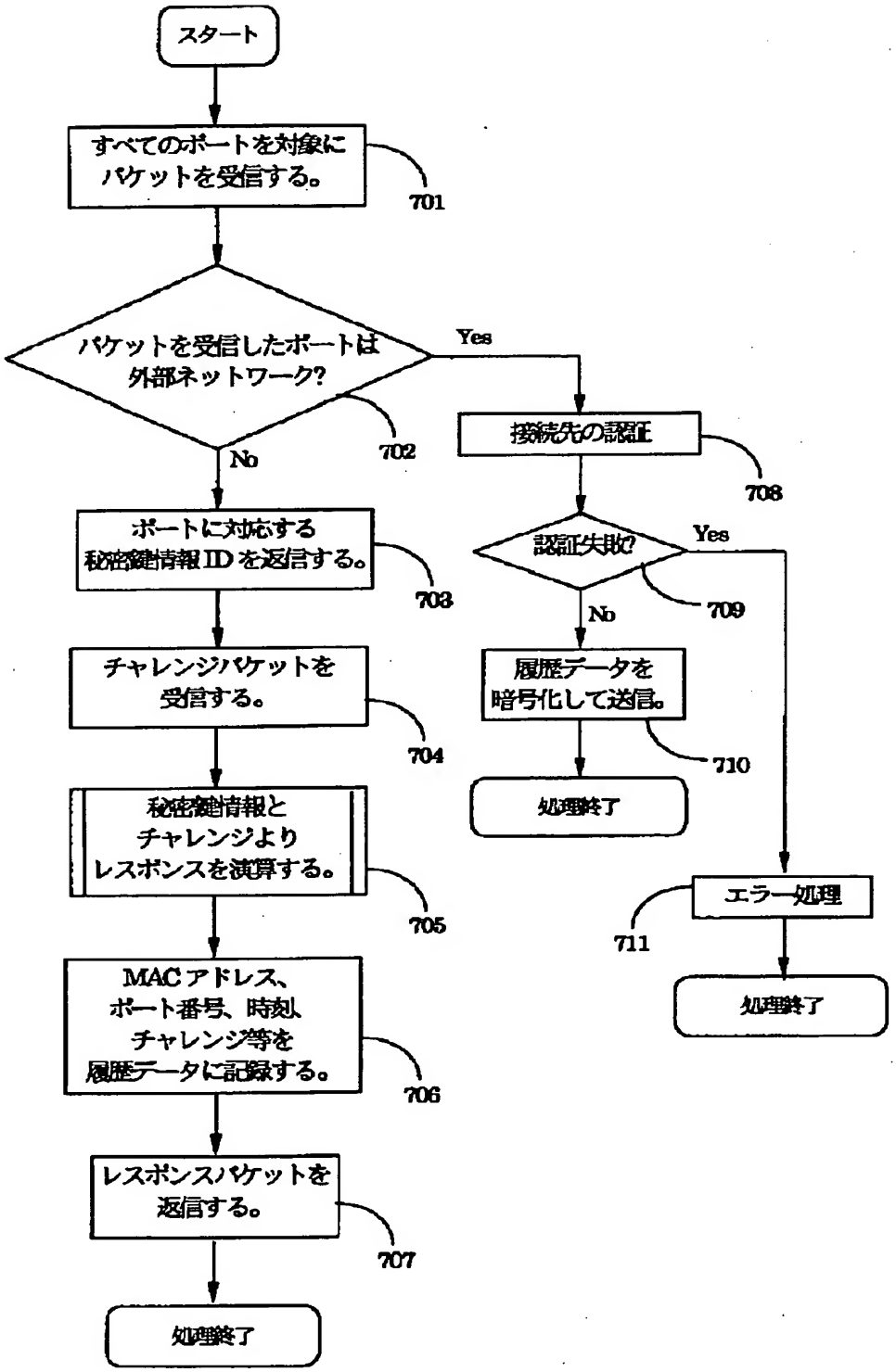
【図１１】



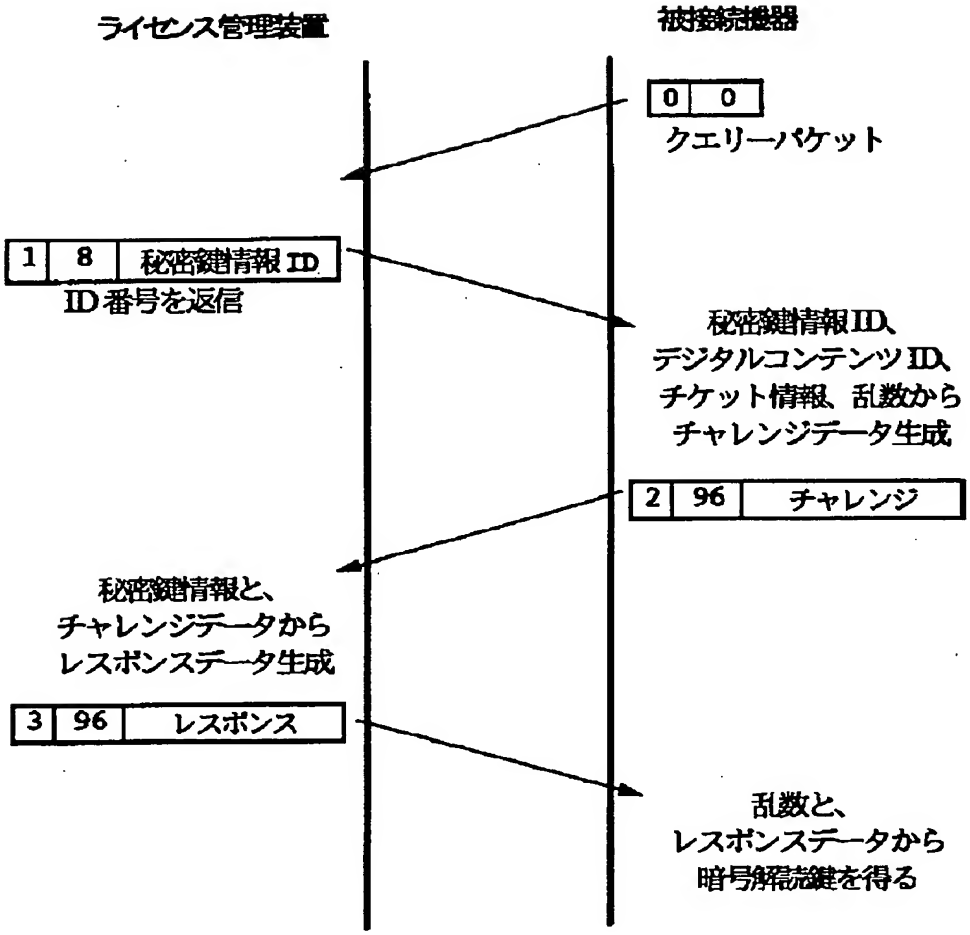
【図５】


スタート
すべてのポートを対象に
パケットを受信する。
501
受信したパケットの
発信元MACアドレスと
受信したポート番号を
経路表に登録する。
502
パケットの宛先は
ブロードキャスト?
503
Yes
No: ユニキャスト
宛先のMACアドレスは
経路表に登録されている?
504
No
受信したポートを除く
全ポートに対して
パケットを同時中継する。
507
処理終了
Yes
発信元ポートと
宛先のポートが同じ?
505
Yes
処理終了
No
経路表に登録されたポートにのみ
パケットを中継する。
506
処理終了

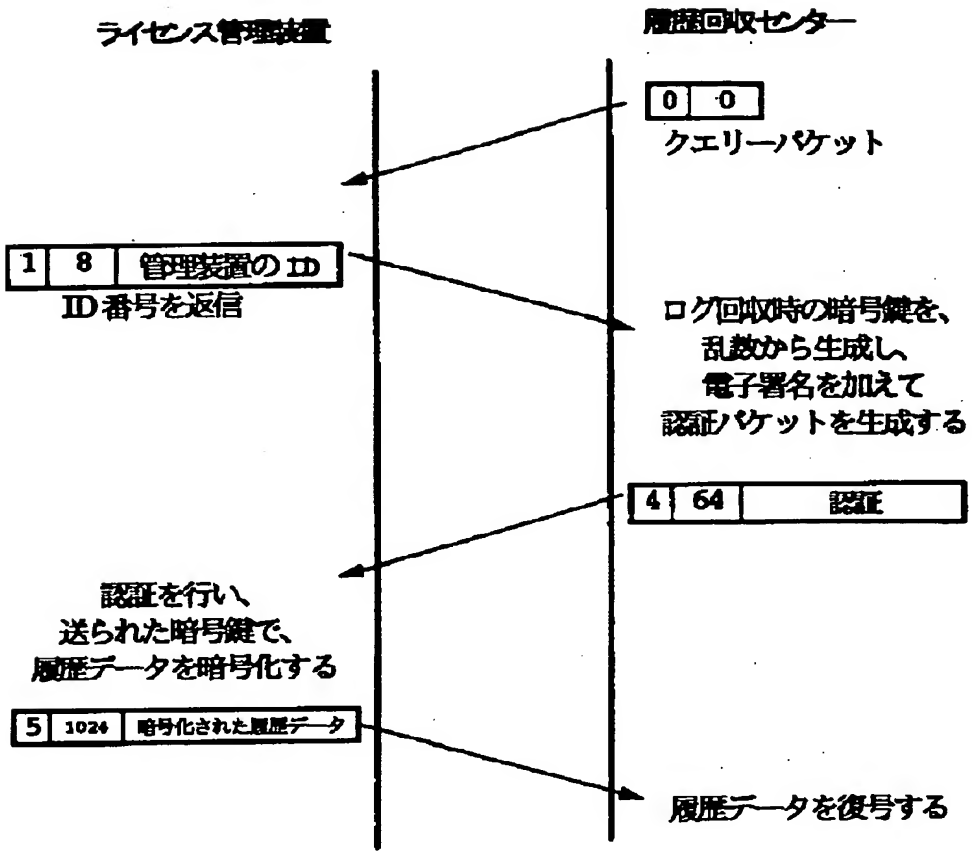
【図７】


スタート
すべてのポートを対象に
パケットを受信する。
701
パケットを受信したポートは
外部ネットワーク?
Yes
No
702
ポートに対応する
秘密鍵情報IDを返信する。
703
チャレンジパケットを
受信する。
704
秘密鍵情報と
チャレンジより
レスポンスを演算する。
705
MACアドレス、
ポート番号、時刻、
チャレンジ等を
履歴データに記録する。
706
レスポンスパケットを
返信する。
707
処理終了
接続先の認証
708
認証失敗?
Yes
No
709
履歴データを
暗号化して送信。
710
処理終了
エラー処理
711
処理終了

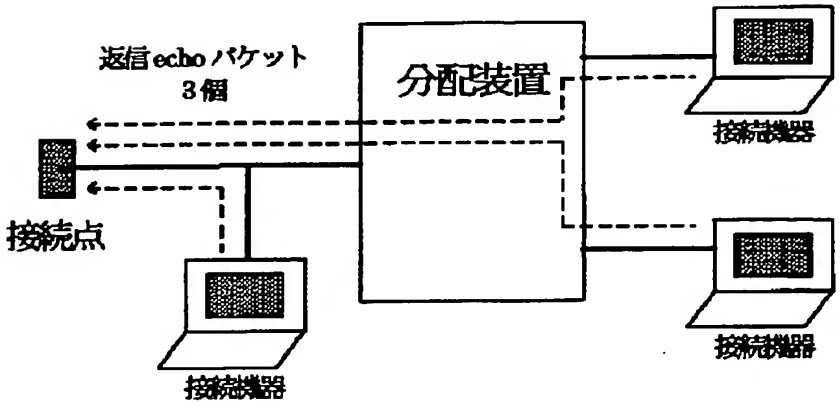
【図８】


ライセンス管理装置
被接続機器
0 0
クエリーパケット
1 8 秘密鍵情報ID
ID番号を返信
秘密鍵情報ID、
デジタルコンテンツID、
チケット情報、乱数から
チャレンジデータ生成
2 96 チャレンジ
秘密鍵情報と、
チャレンジデータから
レスポンスデータ生成
3 96 レスポンス
乱数と、
レスポンスデータから
暗号解読鍵を得る

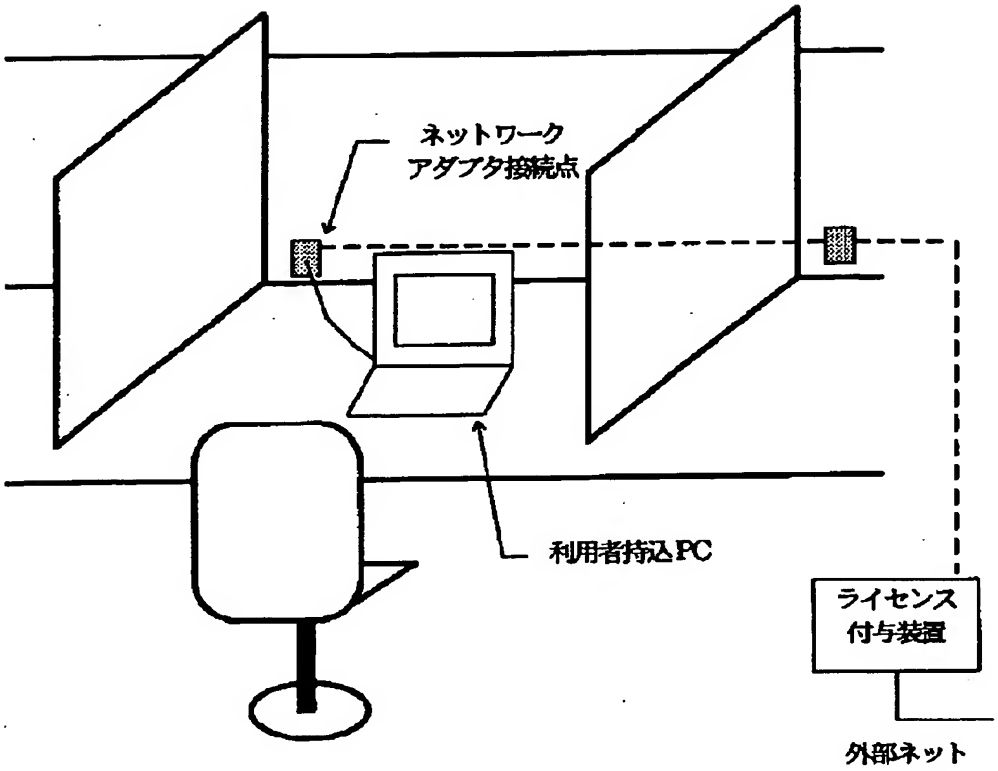
【図１０】


ライセンス管理装置
履歴回収センター
0 0
クエリーパケット
1 8 管理装置のID
ID番号を返信
ログ回収時の暗号鍵を、
乱数から生成し、
電子署名を加えて
認証パケットを生成する
4 64 認証
認証を行い、
送られた暗号鍵で、
履歴データを暗号化する
5 1024 暗号化された履歴データ
履歴データを復号する

【図１２】


返信echoパケット
3個
分配装置
接続機器
接続点
接続機器
接続機器

【図１３】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI			技術表示箇所
12/56			11/20	102	Z	

(72)発明者　大澤　隆
神奈川県足柄上郡中井町境４３０　グリーンテクなかい　富士ゼロックス株式会社内